IT Unit 4

Topic 2

# Information management

**Ch. 6, Security Measures** (Informatics, p 275-280)

Threats to data and information

1. Why is it important to maintain security over an organisation’s data & information? Explain the consequences of failing to maintain security.
2. Accidental threats:
   1. List causes of accidental threats with examples

* Poorly Managed backups: being unable to recover from data loss can caused by poor backup procedures, such as backing up infrequently, inadequate storage media, or a lack of testing of the backup regimen.
* User Error:
* Disclose private information, such as passwords
* Delete vital records or files
* Damage databases
* Damage hardware; for example, by accidentally spilling coffee on a file server
* Invite unauthorised people into secure areas
* Choose weak
* Poor Management:
* Staff who are dismissed may delete files or steal data before they leave
* A disgruntled IT manger may leave without telling anyone the network administrator password, so the company is locked out of its own system
* Employees have unauthorised duplicate keys cut that can be later used to enter the building without authorisation
* Staff are untrained in cases of emergency
* The network resources are wasted in illegal unauthorised purposes, such as downloading torrents
* Security updates are not installed.
* Staff are permitted to use unauthorised or unapproved equipment, such as unsecured wireless access point, unsecured or infected personal laptop ot infected software
* Lost data storage devices
* USB keys are left plugged into public computers
* Portable hard disks or laptops are left in taxis, on public transport or in public places.
* Obsolete computers are sold without first being reformatted
* Unsafe Internet usage
* Porn, gambling, hacking or life sharing can open up an entire network to malware via Trojans or drive by downloads
* Employees may open infected attachments, reply to spam, respond to phishing attempts, click links in suspicious emails, or mistakenly send valuable data to the wrong email address
  1. How can each of these threats be prevented or rectified?
* Poorly Managed backups: Ideally, organisations should backup all their data every day and store their backup’s offsite. They should also test their backup procedures to ensure that they are working properly and backups can be restored. They should also use quality storage media. You should also backup frequency and follow the same procedures, Albert on a smaller scale.
* User Error: Train Staff thoroughly in the use of software, computers and company procedures, such as file naming conventions, and how to choose strong passwords and recognise social engineering
* Poor Management:
* Revoke the network access of employees before they are fired
* Keep a secret master password (unknown to the IT manager) that gives complete access to the digital systems
* Use copy restricted keys or electronic security passes that cannot be copied
* Carry out drills to practice all aspects of the disaster recovery plan
* Use network-monitoring software to detect intrusions a d to log all network activities, such as opening or emailing sensitive documents.
* Enforce policies forbidding the use of unauthorised equipment.
* Lost data storage devices
* Encrypt all portable storage devices
* Reformat or destroy the hard disks of obsolete computers
* Unsafe internet usage
* Use the network proxy servers to block access to all internet sites apart from those needed by staff to do their work

1. Technical threats:
   1. List causes of technical threats with examples.

* Equipment failure
* Failure of servers, hard disks or core communication equipment such as switches and routers can cause loss of access to network data, data loss and loss productivity.
* Computers in humid, hot or dusty conditions tend to fail quickly
* Electric problems
* Blackouts, brownouts, spikes and power surges and damage sensitive electronic equipment.
* Software bugs
* Bugs (programming errors) in an operating system, device driver or application can crash and lose data or make computer vulnerable to attack.
* Improperly configured equipment
* Dangerous security holes or poor performance can be caused by equipment that has been configured incorrectly ; for example, if:

Wireless encryption has not been enabled

* Outdated or incorrect device drivers are being used
* Malware infection
* Once malware enters a system it can spread and expose an entire network to exploitation and data loss. Malware includes worms, Trojans, viruses, spyware, adware, root kits and ransomware
  1. How can each of these threats be prevented or rectified?
* Equipment failure
* Do not buy cheap or underpowered equipment
* Maintain and update hardware properly and handle equipment carefully
* House servers in secure, air-conditioned environment
* Electric problems
* Servers need battery-backed uninterruptible power supplies UPS
* Software bugs
* Regularly update software and operating system
* Improperly configured equipment
* Read the manual. Visit manufacturer forums to learn of problems and cure from other product users
* Malware infection
* Use vulnerability management software to perform automated scans of systems to discover security weaknesses such as open ports, unpatched software and SQL injection vulnerability.

1. Deliberate threats:
   1. List causes of deliberate threats with examples.

* Malicious Staff
* It is a estimated that 18% of deliberate attacks on systems come from staff within an organisations. Of those, half come from digital systems staff. Staff with privileged access may delete data out of spite or steal valuable data to use as a bargaining tool when seeking jobs with a rival company
* Crackers
* Malicious hackers may penetrate systems to plant botnet software or key-loggers so they can control systems remotely to steal data, discover passwords or banking information, conduct DDoS (distributed denial of service) attacks or turn computers into zombies that deliver spam.
* Identify theft
* Once enough personal information is known about victims, their credit cards misused. Victims may make matters worse
* By reusing the same password on different sites
* With carless browsing practices
* Equipment theft
* Thieves may walk off with expensive hardware, along with the irreplaceable data stored on it.
* Vandals
* People may physically damage equipment or electronically deface a website for fun, revenge, fame, money or a challenge.
* Espionage
* Political espionage aims to discover state secrets of a rival nation
* Corporate espionage aims to learn about a competitor new product, business plans, or how much they plan to bid on a government trend
* Fraudsters
* Scammers, phishers and social engineers manipulate gullible staff to gain unauthorised information or payment by trickery.
  1. How can each of these threats be prevented or rectified?
* Malicious staff
* Hire external consultants to conducts security audits and examine networks for
* Secret back door entrances so employees cannot enter system after leaving the company.
* Booby traps that damage the system if employees are aggrieved
* Unauthorised networks privileges, such as staff giving themselves administrator access.
* Crackers
* Constantly scanners, run networks monitoring software to identify attempts to break in.
* Identify theft
* Do not reuse passwords on different sites
* Keep malware scanners up to date
* Avoid suspicious sites, such as gambling, pornography or pirate software sites.
* browse in incognito mode
* carefully check software installations for devious extra software additions, such as toolbars
* use multi-factor authentication whenever it is offered
* Equipment theft
* Improve physical security and strengthen security procedures: for example keep doors locked and do not allow non-staff near company computers
* Record serial numbers of equipment so police can identify stolen equipment
* Encrypt
* Vandals
* Improve physical and electronic security
* Keep your website files backed up
* Espionage
* Encrypt all documents so they are unreadable even if they are stolen
* Run continuous networks monitoring software to detect break-ins
* Fraudsters
* Train staff to recognise deceptive practices

1. Event-based threats:
   1. List causes of event-based threats with examples.

* Natural disasters
* Disasters such as fires, floods, storms, lighting and earthquakes can cause equipment failure and even destruction. While some may be reasonably anticipated based on the time of year and location, such as bushfires in a Victorian summer or an earthquake in Tokyo. Other may completely unpredictable and unexpected, such as the deadly Newcastle earthquake of 1989
* Manmade disasters
* Acts of war, riots, terrorism or civil unrest can cause devastating disruptions to information systems.
  1. How can each of these threats be prevented or rectified?
* Natural disasters
* Conducts backups ensuring that all backups are kept offsite
* Maintain and practise your data disaster recovery plan
* Consider strong data in buildings designed to withstand earthquakes or that are elevated above flood plains
* Manmade disasters
* Monitor the news. With enough early warning data, mangers may have enough time to protect data.